~~CONFIDENTIAL~~

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND 20755

Serial: M503/10382-72
30 November 1972

~~CONFIDENTIAL~~

MEMORANDUM FOR THE CHAIRMAN, COMPUTER SECURITY SUBCOMMITTEE OF THE SECURITY COMMITTEE, USIB

SUBJECT: Security Level of COINS

1. The NSA has carefully assessed the proposal to incorporate TK information in the COINS net as proposed by the DIA Member. In the assessment of this proposal, the NSA has determined that there is a possible alternate solution to this problem. It appears feasible for NSA to implement the proposal on RYE utilizing existing security mechanisms in this system. Briefly, we submit that selected RYE terminals in NSA could be authorized access to a COINS TK data base through execution of the RYE security features. Although no formal security test and evaluation of the RYE System has been conducted, the system has been operating under this security structure since 1967, and experience has shown an insignificant amount of misdirection of output. We feel confident that this security structure reasonably insures data only going to those terminals authorized for such access.

2. It appears that few if any additional TK billets would be necessary to accommodate the above proposal within NSA.

3. The NSA further recommends that the DIA execute those recommendations expressed in the DIA On-Line System Test and Evaluation Report of 1 August 1972. Essentially, this involves dedicating one of the Honeywell 635 Processors to the COINS environment and the ISS internal processing of DIA. It would be necessary for the DIA to remove all compiler language capability from the processor and only afford the user the two Information, Storage and Retrieval languages necessary to access the ISS and COINS data bases.

4. The COINS Security Officer has conducted a thorough examination of the Intelligence Data Handling System Communications (IDHSC) and has determined that the subscribers to this net are in effect a communications interface with the COINS network. There are no files or data bases housed within the IDHSC network and the dedicated IBM 360-30 PACOM Switch is utilized as a store and forward process for IDHSC queries to the COINS network in the Washington, D. C. area. The COINS Security Officer recognizes that there are some personnel administrative problems regarding

~~CONFIDENTIAL~~

Classified by DIRNSA (NSAM 123-2)
Exempt From GDS, EO 11652, Cat. 2
Declas Date Cannot Be Determined

additional TK billets to be authorized the IDHSC environment. He suggests that the DIA examine this problem on an expeditious basis and provide the number of billets required to the IHC of USIB. DIA should also formally state their position regarding the future use of the Honeywell 635 in the COINS network.

5. Plans are currently underway, through the auspices of the COINS Security Panel, to incorporate need-to-know controls within the COINS net at the earliest possible date.

6. With the execution of the above described proposal, it would then provide for an environment in which the COINS TK test could be conducted. The results of the test will provide for a quantitative measurement for deciding the future of a TK data base in the COINS.

7. The NSA urges that this proposal be given serious consideration and further evaluation.

25X9

[redacted]

PL 86-36

Computer Security Subcommittee
Security Committee, USIB

3 Incls:
1. Plan for the Simulated TK Test of the COINS Network, dtd 21 Mar 72
2. Memo for the Chairman, USIB Security Committee, dtd 10 Nov 72
3. Draft Memo to Chairman, IHC, dtd 10 Nov 72

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND 20755

Serial: M503/10382-72
30 November 1972

CONFIDENTIAL

MEMORANDUM FOR THE CHAIRMAN, COMPUTER SECURITY SUBCOMMITTEE
OF THE SECURITY COMMITTEE, USIB

SUBJECT: Security Level of COINS

1. The NSA has carefully assessed the proposal to incorporate TK information in the COINS net as proposed by the DIA Member. In the assessment of this proposal, the NSA has determined that there is a possible alternate solution to this problem. It appears feasible for NSA to implement the proposal on RYE utilizing existing security mechanisms in this system. Briefly, we submit that selected RYE terminals in NSA could be authorized access to a COINS TK data base through execution of the RYE security features. Although no formal security test and evaluation of the RYE System has been conducted, the system has been operating under this security structure since 1967, and experience has shown an insignificant amount of misdirection of output. We feel confident that this security structure reasonably insures data only going to those terminals authorized for such access.

2. It appears that few if any additional TK billets would be necessary to accommodate the above proposal within NSA.

3. The NSA further recommends that the DIA execute those recommendations expressed in the DIA On-Line System Test and Evaluation Report of 1 August 1972. Essentially, this involves dedicating one of the Honeywell 635 Processors to the COINS environment and the ISS internal processing of DIA. It would be necessary for the DIA to remove all compiler language capability from the processor and only afford the user the two Information, Storage and Retrieval languages necessary to access the ISS and COINS data bases.

4. The COINS Security Officer has conducted a thorough examination of the Intelligence Data Handling System Communications (IDHSC) and has determined that the subscribers to this net are in effect a communications interface with the COINS network. There are no files or data bases housed within the IDHSC network and the dedicated IBM 360-30 PACOM Switch is utilized as a store and forward process for IDHSC queries to the COINS network in the Washington, D. C. area. The COINS Security Officer recognizes that there are some personnel administrative problems regarding

Classified by DIRNSA (NSAM 123-2)
Exempt From GDS, EO 11652, Cat. 2
Declas Date Cannot Be Determined

additional TK billets to be authorized the IDHSC environment. He suggests that the DIA examine this problem on an expeditious basis and provide the number of billets required to the IHC of USIB. DIA should also formally state their position regarding the future use of the Honeywell 635 in the COINS network.

5. Plans are currently underway, through the auspices of the COINS Security Panel, to incorporate need-to-know controls within the COINS net at the earliest possible date.

6. With the execution of the above described proposal, it would then provide for an environment in which the COINS TK test could be conducted. The results of the test will provide for a quantitative measurement for deciding the future of a TK data base in the COINS.

7. The NSA urges that this proposal be given serious consideration and further evaluation.

[redacted] 25X9

NSA Representative
Computer Security Subcommittee
Security Committee, USIB

PL 86-36

3 Incls:
1. Plan for the Simulated TK Test of the COINS Network, dtd 21 Mar 72
2. Memo for the Chairman, USIB Security Committee, dtd 10 Nov 72
3. Draft Memo to Chairman, IHC, dtd 10 Nov 72

21 MAR 1972

PLAN FOR SIMULATED TK TEST OF THE COINS NETWORK

1. Purpose

The purpose of this memorandum is to present a plan for testing the adequacy of the COINS network security controls in handling two or more categories of Sensitive Compartmented information.

2. Objective

The objective of the test is to exercise in the various nodal systems the security controls designed to maintain separation of different categories of compartmented data as a prelude to incorporating TK material in the COINS system.

3. Scope

The test will run for 30 days and involve all nodal systems, primary users, secondary users (e.g., CONAD), and non-COINS terminals or systems attached to COINS nodal systems.

4. Clearance of Personnel

Clearance of Personnel operating all components of the COINS network, other than remote terminals, must be access approved for all Sensitive Compartmented Information contained within the system. Remote terminal users must be cleared for access to all possible types of outputs that the specific remote terminal in use is approved to handle.

5. Responsibilities

Each nodal system will contribute a simulated TK file and a simulated SI/TK file for the test. These may be real files renamed or copied and renamed for the purpose of the test, or test files as the requirements of the participating agencies permit. The agency supplying the files will provide all other agencies with the name of the simulated files, and a description of their content.

Each agency will be responsible for conducting tests as outlined below, and providing test statistics and audit trail records for evaluation.

Incl 1

6. Test Procedures

a) The network will continue in its present SI environment during the test period.

b) It is intended that all routes, all nodes, and all users and attached terminals be exercised in this test. Both COINS and non-COINS terminals are to be used where applicable. It is the intent of the test to test the environment in each agency as it exists. Consequently, only those test patterns possible in each agency at the time of the test must be exercised. The test patterns specified include cases that may eventually be incorporated as COINS network operations (e.g., having TK-only users referencing TK-only files) and is not limited to the original COINS charter. Inclusion of these cases does not necessarily imply that these modes of operation must or should be initiated. Rather, they are included as a very simple extension of the basic premise of the network and the specific objective of this test.

c) Routes: The following routes will be tested for each of test patterns in 6c.

TO FROM	NSA	DIA	NPIC	
NSA	X*	X	X	
DIA	X	X*	X	
NPIC	X	X	X*	
STATE	X	X	X	
NIC	X	X	X	
CIA	X	X	X	
CONAD	X	X	X	
EXTERNAL**	X	X	X	

*Local use of COINS files.

**For those systems having an external system/terminal attached (e.g., AFNIN to DIAOLS), the tests will involve attempting to gain access to COINS, and if possible or permitted, then the other tests indicated. (By 'external,' we mean actual or potential COINS subscribers who are not specifically enumerated above, but who are or may be COINS users in the near future. External users do not contribute or maintain files in COINS.)

d) Test Patterns: The following test patterns will be run. The correct system for response to the test type is indicated-- R for Reject, A for Accept

TERMINAL/ (USER) TYPE \ COINS FILE TYPE	SI	SI/TK*	TK*	COLLATERAL
COINS AUTHORIZED				
SI	A	R	R	A
SI/TK	A	A	A	A
TK	R	R	A	A
COLLATERAL	R	R	R	A
NON-COINS AUTHORIZED				
SI	R	R	R	R
SI/TK	R	R	R	R
TK	R	R	R	R
COLLATERAL	R	R	R	R

*SIMULATED

e) Tests: The test will consist of queries directed to each of the test file types indicated above. For those systems that permit redirection of the output to other than the terminal making the request, the tests will include attempts to output the results of a proper query to an unauthorized terminal. Each nodal system will also conduct part of the test from "privileged" terminals if such exist in the system. (The results should remain the same.) Where multifile queries are permitted, the test queries will include combinations of authorized and unauthorized files. 'External' users of COINS at the time of the test (as defined above) are required to participate in the test. New external users, coming into the network subsequent to the test, will conduct the test from their terminal(s) prior to joining the network. Audit data and listings of their tests will be made available to the COINS project office for review prior to accepting them as COINS users.

f) At the current network activity level, it has been estimated that 1ØØ test queries from each source point to each destination will give sufficient data that would, if no mishandling of the data occurs, give a 99% confidence that the controls are working properly and are capable of maintaining the separation of different categories of information desired. This amounts to 5 queries to each destination point per work day for the one month test planned.

7. General

Outlined below are ways that each participating COINS member may participate in the test and provide beneficial test results for security evaluation at the conclusion of the COINS simulated TK test.

A. Each member will provide a test platform that will generate sufficient data for a security evaluation of the COINS system.

B. In the event of a "Security Violation" or spillage occurrence, which might violate the need to know for compartmented information, the proposed test utilizing simulated TK material will continue for the purpose of determining if there might be more than one odd occurrence of the problem. This will allow the continued building of the data base for evaluation purposes.

C. It is suggested that the method of testing from either a selected few or all remote terminals be as follows. When a query is made to the regular COINS FILENAME, a query should also be generated in the exact same makeup except that the COINS (TEST) FILENAME is used; i.e., two identical queries except for the FILENAME.

D. The nodal systems should have all of the intended TK and SI/TK Hardware/Software controls applied in the operational mode at the beginning of the test period so that if a favorable test analysis results, no additional changes will be required to the COINS network to bring into active use standard TK and SI/TK compartmented files.

E. During the proposed 3Ø day TK,test information from the AUDIT TRAIL produced by each COINS members system or subsystems should be submitted to the COINS Project Manager on a weekly basis.

F. Each agency will insure that all terminal users of their COINS nodal system are informed that a COINS test is being conducted, and that it is imperative that any unusual occurrence or output be promptly reported in accordance with the COINS Operating Procedure No. 5 dated 1 August 1971.

G. In the event that the individual COINS member audit trail procedures do not provide the information listed in paragraph 8, manual logs should be instituted. The same reporting procedures specified should be followed with the manual logs.

8. Audit Trails

The following audit trail information should be provided; however, the listed items should not be considered as the only items useful for security evaluation of this COINS test.

A. User identification or terminal identification shall be provided to the extent there is no ambiguity as to what user or what terminal performed the operational query. There should be an indication as to whether any verification process took place automatically within the computer or was accomplished manually (such as password verification).

B. The date of access, time of entering the system, time out of the system and possibly the amount of CPU time used should be made available.

C. What file was accessed, or attempted to be accessed, and either success or failure noted. The number of attempts before entry or the number of attempts before being "dumped" from the system should be logged.

D. If a file is accessed, what functions were performed if authorized, or what functions were attempted to be performed if they were illegal or non-authorized operations from either the terminal, the user, or to the file--e.g., an attempt to write on a read only file should say, Attempt to write::: NOT AUTHORIZED:::

E. A listing of terminal locations and the security level of those terminals and/or their authorized areas should be available for analysis purposes if not contained in the Audit Trail for the users COINS terminals.

F. Finally, but not necessarily least, is the fact that the Audit Trail should also contain notations of any exceptions to any of the established normal procedures, attempted illegal entries (to either the system or to files), attempts to perform illegal functions such as delete, write, or read/write, and attempted illegal outputs to either terminals or users.

9. Evaluation

Evaluation will be made by the COINS project office aided by members of the COINS security panel as required. During the test period, the panel will meet at the halfway point to determine the progress of the test, and recommend any modifications to the test procedures or duration of the test.